JCA-NET セミナー
5 月暗号化ソフトの導入——政府の通信情報収集への対抗手段として

2026/5/27

としまる
toshi@jca.apc.org

「ここでの教訓は、わたしたちが法律で自衛するだけでは不十分だということだ。わたしたちは数学でも自衛する必要があるということだ。暗号は重要すぎて政府だけに任せておくことはできない」

ブルース・シュナイヤー『暗号技術大全』（※）

※ 山形浩生訳、ソフトバンクパブリッシャーズ、 2003(原書 1996)

シュナイアーはこの発言を後に『暗号の秘密とウソ』で自己批判します。暗号だけでも防衛できない、ということを悟ったからです。つまり、暗号技術には多くの限界もある、ということなのですが、これは、だから暗号は効果がない、とか無意味だ、ということではありません。法だけでもダメで、暗号も含めたもっと様々な対処をしないと政府の監視に対処できなくなった、ということです。法が敵の武器になるなかで、暗号技術はその重要性を増していますが、そでだけでもダメだとシュナイアーが言うとすれば、何が足りないのでしょうか。皆さんは何だと思いますか？

セミナーの核心にあたる課題は、スパイ機関の創設など私達を監視する政府の機関をめぐる法律に対して、法案を阻止することができさえすれば、それで私たちのコミュニケーションの権利がまもられる、ということにはならない、ということです。ましてや新規のスパイ機関関連の法律が成立した場合はなおさらです。

しかし、**法律がどうあれ、私たちには、対抗手段がある、というところがセミナーの中心的なテーマです。**この対抗手段をとることは必須になります。もちろん対抗手段は万能でも完璧でもありませんが、何もしない、という選択は、たぶん、自分だけでなく、自分とコミュニケーションをとる人々をリスクに晒す可能性があります。

対抗手段の有力なもののひとつが暗号化です。しかし、万能でもないし他にすべきこともあります。自分で暗号化を工夫することは、自分の家の戸締りを警察に委ねずに、自分で対処する、ということに似ています。戸締りさえすれば安全、ということでもないのは、インターネットやコンピュータ・コミュニケーションでも同じです。

前回のセミナーの内容の反省と参加された皆さんの質問などを踏まえて、27日のセミナーでは、告知文の参考資料として紹介したグレンコラ・ボラダイル「反対派を防衛する―社会運動のデジタル弾圧と暗号による防御」を中心にして説明することにします。
前回のセミナーに参加された方から「そもそも暗号自体がよくわからない」という感想もいただきました。以前ボラダイルの小冊子を紹介してセミナーをやったこともありますが、うまく全体を網羅することはできませんでした。今回は、この小冊子を紹介しつつ必ず読んでほしい箇所と、飛ばしてあとで読むのでも構わない箇所を私なりに取捨選択して紹介します。
本書の日本語版は下記にあります。自由にダウンロードできます。
https://jca.apc.org/wp-content/uploads/2026/05/反対派を防衛する統合版.pdf

本書は、社会運動に関わる人々を対象に、インターネット時代に急速に拡がりはじめている捜査機関による監視やネットへの取り締まりによる運動への弾圧に対抗するための基本となる考え方と、実践的な取り組みについて、週末や休日に読み切ることができる長さを念頭に置いて書かれたものです。

著者は、コンピュータサイエンスの専門家であると同時に、活動家でもあり、米国の活動家が大量監視と巧妙な監視技術によって日々直面しているリスクにを深刻に受けとめ、セキュリティの専門家ではない人達にも必要な最低限の知識と情報の提供を念頭に置いています。



訳者前書き

本書の意義について書いておきます。本書の特徴は、書名の副題にあるように、**コンピュータ・コミュニケーション領域で進展しつつある警察などによる弾圧技術の高度化を念頭に、高度化する弾圧への対抗手段の確保**です。プロバイダーなどが保有するデータへの警察のアクセスは頻繁に行なわれています。また、スマホやパソコンは押収されれば確実に内部のデータやクラウドのデータを取得されると考えなければならないでしょう。 AI 、生体認識技術、ビッグデータ利用が進むなかで、ネットワーク盗聴、ネットでの活動の追跡や行動予測が進歩し、私たちの体感では捕捉しづらい手法で私たちの基本的人権が侵害されています。こうしたなかで、本書は、私たちの防御の手段の核心に「暗号」を据えました。監視や盗聴から私たちのコミュニケーションを防衛する最後の砦が暗号です。**暗号技術を駆使することによって、たとえ、デバイス [パソコン、スマホなど] が押収されたり盗聴・追跡されたり、契約しているプロバイダーが捜査機関に協力したりしても、データを解読することはできず、私たちの行動の監視を防御することも可能になります。**内部告発者が告発の証拠をジャーナリストに渡す場合も、人権活動家が弾圧を回避して支援する場合も、**暗号技術なしには、私たちのリスクを最小化することはできません。完璧とはいえないとしても、暗号は私たちのセキュリティにとって必須のものなのです。**このことを本書は、技術の仕組みから現実の運動での活用まで、平易に説明しています。事例は米国のものですが、日本にも十分あてはまるものです。日本では社会運動の担い手たちが暗号の重要性を運動の文化にとっての共通認識にすることがますます必要になっています。この意味でも本書は重要な意味をもつと思います。

はじめに　なぜデジタルセキュリティなのか？

2013 年夏、エドワード・スノーデンは、米国家安全保障局（ NSA ）、米中央情報局（ CIA ）をはじめとする世界各地の 3 文字機関の大量の文書を公開し、世界を震撼させました。この 1 年以上の間、これらの機関のデジタル情報収集能力の高さ、特に米国の情報収集能力の高さが、毎日とは言わないまでも毎週のように明らかにされました。 NSA は、インターネットや電話のネットワークを介して、暗号化されていないあらゆる情報に加え、弱い暗号化が施された情報や、企業のサーバーで暗号化されていない情報も入手できているように感じられました。その感覚は真実に近いものがあります。当時、私は環境保護活動に従事しており、社会運動が歴史的にスパイ活動による国家弾圧に苦しめられてきたことを知っていました。 **NSA や CIA が収集できる情報の量が多ければ多いほど、国家による弾圧はより簡単で効果的なものになります。国家があなたの活動についての情報を知れば知るほど、あなたの目的を妨げることが容易になります。**だから、私は心配だったのです。気候変動に立ち向かうために活動しているすべてのグループに不利な状況のなかで、私たちは気候変動に立ち向かえるのだろうか？組織的な人種差別についてはどうだろう？私たちに希望はあるのだろうか？スノーデンの暴露から間もなく、私は市民的自由防衛センター（ CLDC ）と提携しました。 CLDC の法律研修を補完するために、私は活動家向けのデジタルセキュリティ研修を定期的に開催するようになりました。この研修では、大量監視が行われている現代社会において、修正第 1 条 [信教、言論表現の自由] および修正第 4 条 [不当な捜査・逮捕等されないこと] の権利を守るためには、暗号化が唯一の方法であるという前提に立っています。この本は、こうした教育活動から生まれたものです。

本書の構成

第　1　部　暗号技術の紹介

暗号技術の基本。
例示では、アサタがボビーと通信し、エドガーがそれを盗聴している、という例を用いる。
アサタ・シャカール　：（ 1970　年代前半に）黒人解放軍やブラックパンサー党のメンバー
ボビー・シール：公民権運動時代のブラックパンサー党の共同創設者
J.　エドガー・フーバー　： FBI 設立者で監視や抑圧の責任者

第　2　部：デジタルによる社会運動の弾圧（米国の場合）

1.　米国では歴史的に社会運動がどのように抑圧され監視がどのような役割を果たしているのか。
2.　米国でどのような監視システムやその他のデジタルな脅威が使われているか。

第　3　部：社会運動を守るために（アメリカ編）

脅威の分析、情報を防衛するためのツールの分類など。特定のツールを利用できるかどうか、あるいはそれに関連するリスクは、あなたの政治的背景によって異なる。

例えば、中国のように検閲が行われている国では、 Tor （匿名性を提供するインターネットブラウザー）の使用が難しくなる場合があります。

今回は第２部⇒第３部⇒　第１部の順で話をします。

以下は本書の結論に記載されている項目です。これらについて既にごぞんじであれば、本書を読む必要はないかもしれません。

01 必須の基準

1.　エンド・ツー・エンドの暗号化
2.　中間者攻撃を防ぐ機能
3.　オープンソースを選択
4.　アプリの真正性を暗号署名で検証できる

02 追加の望ましい技術的基準

1.　デジタル・セキュリティ・ツールは、クロスプラットフォームが望ましい
2.　セキュリティ監査を受けている
3.　匿名性や仮名性を提供している
4.　ツールの設定確認（暗号化が選択できれば、選択する）
5.　ピア・ツー・ピア通信やフェデレーション機能の利用（中央集権的に特定の企業がサーバーを管理しない仕組、あるいはサーバーを介さない仕組み）

03 技術以外の基準

1.　プロバイダが採用した財務モデル。ツールが無料で使えるとしたら、その理由を知るべき
2.　ツールが運動志向の場合、それはプラスにもマイナスにもなり得ます。サーバーの運営主体が社会運動団体の場合は、サーバー内での暗号化ができていなくても信頼性が高い。（riseup の jitsi-meet）
3.　事業者の透明性

結論
デジタルセキュリティツールの選択

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

社会運動に対するデジタルの脅威

二つのテーマ
1．　米国政府はどのようにして社会運動を抑圧しているのか
2．　政府の対敵諜報プログラムとは何だったのか、

米国には、自国を含めて社会運動、特にリベラルや左翼的な社会運動を抑圧するという形で干渉してきた長い歴史があります。

労働者の組織化、独立運動、公民権運動、環境保護運動などが、しばしば大企業の要請や協力を受けた米国政府の敵視政策に遭ってきました。

社会運動がデジタル・セキュリティに無頓着だったらどのようなリスクがあるのでしょうか。ここでは過去に国家がどのように社会運動を妨害してきたかを見ると役に立ちます。このような歴史を知ると、ときには圧倒され、過去に敵対者とみなされたり、国家が実際に敵対している人々に対して使用できるデジタル的に強化されたツールが増えていることで無力感を抱きがちですが、対抗手段はあることを本書は教えています。

ここでは過去に国家がどのように社会運動を妨害してきたかを見ると役に立ちます。

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

抑圧の手口

1．　直接的な暴力
殴打、爆撃、銃撃、その他の形態の暴力が、国家やその他の機関、権力側組織によって反体制市民に対して行われます。このような直接の暴力には、大きな集団に対する制圧や、標的を絞った暗殺の例があります。控えめに言っても、これらの行為は、**生命や身体への恐れを生じさせ、社会運動への参加を妨害するもの**です。

2．　法制度
嫌がらせ目的の逮捕、訴追、尋問、あるいは特別な法律を使って偏見のあるやり口で個人に干渉する、といった法制度が存在します。国家は、しばしば**虚偽の微罪で活動家を逮捕**したり、長い間適用されたこともないあいまいな法律を根拠にしたりして活動家を逮捕したりしており、差別的な法的迫害の枠組を悪用しています。

3．雇用の剥奪
政治的信念や活動が原因で、雇用を脅かされたり、実際に失ったりすることがあります。反体制派の中には、政治的信条を理由に、そもそも雇用に至らない人もいます。雇用の妨害は一般的には雇用主が行うものですが、国が直接・間接的に強力な影響力を持つこともあります。

4．あからさまな監視
あからさまな監視をする目的は、情報収集ではなく、威嚇です。（情報収集なら秘密裏にするほうが効果的ですから。）これは、報復を恐れて言論を控えるという萎縮効果をもたらすことを目的としています。

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

抑圧の手口（続き）

5．秘密の監視
標的を絞った監視の手段には、**スパイの侵入、特定対象の盗聴、データ提出命令や令状**などが使われます。潜入者（対象グループのメンバーになりすました隠密エージェント）、情報提供者（グループのメンバーから金銭や脅迫で情報を引き出す）の利用などもあります。また、インターネットの監視や郵便の開封など、大量監視技術によって得られた個人や集団の情報を収集し、保存し、分析するなどによっても監視対象が広範に及ぶことがあります。

6．　騙し
“濡れ衣”密告者ジャケッティング　Snitchjacketingとは、多くの場合潜入者の工作によって、**本物の活動家に対して政府への密告者だとかグループに悪意を抱いているなどの疑念を組織内部に植え付ける**ことをいいます。単にグループの活動を当局へ報告するのではなく、グループに暴力や違法な活動・戦術を促す役割を持った潜入者は、**かく乱工作員**と呼ばれ、グループを法的危機に陥れたり、グループの信用を失墜させせたりする活動を行います。**“虚偽のプロパガンダ“**とは、活動家の組織の間に分裂を誘発させせたり、連帯を損なったりする目的で文書をでっちあげることを意味します。

7．マスメディアの影響
（1）政府が作成した記事をそのまま、あるいは若干の修正を加えだだけで掲載する政府寄りの報道関係者を利用する「**ストーリー・インプラント**（記事注入）」
（2）ジャーナリストや編集者を脅して不要な情報が掲載されないよう圧力をかける「**ストロング・アーミング**（力ずく）」
マスメディアは反体制派を、非常識だ、尋常ではない、危険だなど、社会の主流から外れたものとして描く。これは陰謀によるよりも、ジャーナリズムの規範や価値観を映していることが多いのです。

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

情報技術による妨害

抗議活動中にインターネットやモバイルネットワークへの**アクセスを遮断**したり、特定のサイトや特定の種類のインターネット通信だけを遮断したり、社会運動グループの**ウェブサイトを閉鎖**したりすることなど。
政府は、国レベルでインターネットへのアクセスを遮断したり（抗議活動を抑制する手段として、イランで1週間にわたってインターネットを全面的に遮断した例など）、特定サイトへのアクセスを制限したりすることで知られています（中国のグレートファイアウォールがGoogle、Facebook、 Twitter、 Wikipedia を遮断した例など）。米国の企業もこれに参加し、外国での検閲に「協力」しています。 Zoom（ウェブ会議サービス）は、天安門事件のメモリアルとしてのオンラインイベントを計画していた3人の活動家のアカウントを、中国政府の要請に応じて停止しました。

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

社会運動に対するデジタルの脅威

社会運動が権力者、権力組織、あるいは社会構造に挑戦するとき、**広範囲にわたる監視リスク**に直面します。ひとくちに脅威といっても、それが技術的にどのくらい洗練されているのか、脅威の可能性がどのくらいあるのか、被害の可能性がどのくらいあるのかには大きな違いがあります。**脅威のモデル化とは、運動組織や個人が敵対する相手の範囲を検討し、様々なデータやデバイスが攻撃の犠牲になる可能性を推定し、攻撃された場合の被害についても検討するというプロセス**をいいます。



自分の身を守るために、次のような順序で監視について考えていきます。

01 あなたの敵は誰か。

ブラック・ライヴズ・マターの看板を庭に掲げたことであなたに復讐する近所のネオナチでしょうか。パイプライン反対運動を抑えようとする石油会社でしょうか、内部告発を阻止しようとしている米国政府でしょうか。敵対者が誰であるかを理解することで、敵対者のリソースと能力を推測することが可能になります。

02 敵対者は特にあなたに狙いをつけているのか

あるいは、あなたの正体を突き止めようとしているのか、それとも大量の情報を集めてそこからあなたに関する情報を得ようとしているのか。敵対者はどのような監視戦略をとっているのでしょうか。このような考察から、どのようなデータが、どこで危険にさらされる可能性があるのかを理解することができます。

03 目的のデータを得るために、敵対者はどのような監視手段を採用するでしょうか。

このことを知っておくと、そのデータを保護するにはどうすればいいのかを理解するのに役立ちます。

私たちは敵対者による監視リスクから検討を始めますが、これは戦略的にそうすべきだからです。完璧なデジタルセキュリティを実現することはできませんが、監視から身を守るためにどこに労力を費やすべきかを賢く判断することならできます。

自分の身を守るために、次のような順序で監視について考えていきます。

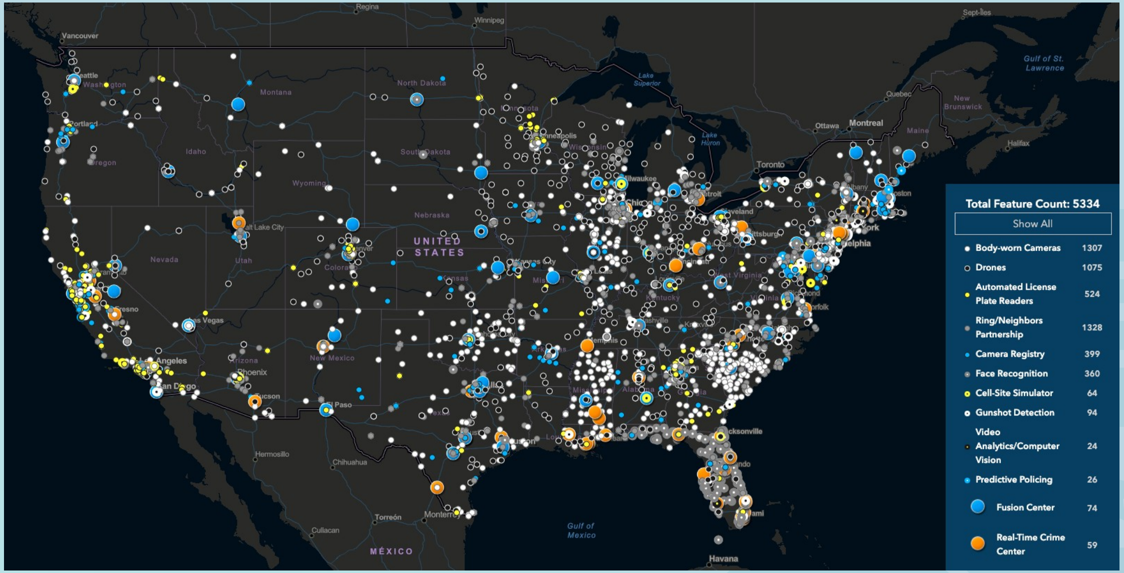
デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

監視を仕掛けてくる敵対者

国家は、監視能力が無限であるかのように見えるが、**強力な暗号を解読することはできない。**最も高度な監視能力を持つ組織として、米国家安全保障局（NSA）がある。2013年にエドワード・スノーデンが公開した情報は、国家レベルの能力を最も包括的に示すものです。

大企業や地域の警察は、互いに情報を共有していますが、必ずしも国家クラスの監視能力が使えるわけではありません。しかし、電子フロンティア財団の Atlas of Surveillance のスクリーンショット（右図）に示されているように、監視を支援するテクノロジーは警察などの司法機関では広く使われています。



https://open.oregonstate.education/app/uploads/sites/137/2021/03/atlas-of-surveillance.png

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

監視戦略

集団監視では、集団全体から情報を収集します。これは、その集団をよく知ることを目的として行われます。例えば、健康関連データを収集・分析することで、新たに発生した病気を特定したり監視したりすることができます。また、集団監視は、一群の監視対象者の中から対象となる人物を特定するための戦略として用いられることもあります。

例えば、防犯カメラの映像を利用して、物的損害を与えた人を特定することができます。また、集団監視によって、特定の個人に関する情報を収集することもあります。例えば、ナンバープレート・カメラを大量に配置して収集した情報をもとに、特定の個人の動きを追跡することができます。

標的監視は、個人または少人数のグループに関する情報だけを収集します。例えば、盗聴は、特定の個人の通信を傍受するものです。もっとも、警察などが誰かのメールを傍受するときは事前に正当な理由に基づく令状を取得する必要があり、ある程度確実な容疑が存在するときに監視が限られるはずで、憲法違反が横行しないように抑制されることにはなっています。

デジタル時代においては、標的監視の手法が大規模に展開されることが多い。

デジタルによる社会運動の弾圧（米国の場合）

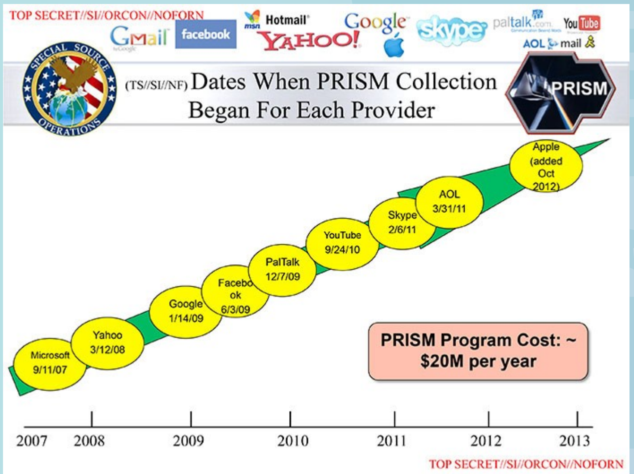
社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

監視戦術

大規模な傍受とデータの収集
2013 年にエドワード・スノーデンが公開した情報の一部として、多くの大規模な傍受プログラムが明らかになりました。STORMBREW、FAIRVIEW、BLARNEY の 3 つのプログラムは、NSA が通信会社と提携し、海底ケーブルを通過するデータをすべて収集するものです。ただし、電子メールやクラウドストレージ内のファイルなど、**通信途上で一般的に暗号化されるコンテンツについては、これらのプログラムでは見ることができません。**

PRISM プログラムは、NSA とさまざまなインターネット企業（Google、Microsoft、Facebook など）が提携し、**企業のサーバーに保管されているデータに NSA がアクセスできるようにするもの。**

情報が送信中に暗号化されていて、STORMBREW、FAIRVIEW、BLARNEY で収集できない場合、NSA は PRISM を介して情報を入手することができます。ただし、**協力企業のサーバー上でもユーザーが管理する鍵で情報が暗号化されている場合はこの限りではありません。**



デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

データの集約と分析

データマイニング
最も基本的なのは検索機能です。つまり、大量のデータから、特定の人物に関連するデータなど、興味のあるデータを取り出すことができます。**XKEYSCORE** は、NSA が蓄えた大量監視データ保管庫を対象とした**検索機能**

Dataminr 社は、一般に公開されているデータ（ソーシャルメディアの投稿など）を**検索**し、自動（ソフトウェア）および手動（人間による分析）の両方の手段を用いて、新たに発生した "危機" （COVID-19 の最新情報やジョージ・フロイドの抗議活動など）の詳細を明らかにし、報道機関、警察、政府などの顧客に提供する。

Palantir は、特定の交差点、特定の地区、特定の個人など、どこで取り締まりすることが必要なのかを**予測**。予測型取り締まりプラットフォームは、現在の警察データを出発点としており、過去に警察が取り締まりをした場所に警察官を派遣する傾向があります。しかし、有色人種のコミュニティや貧困地域は、特に過剰な警察活動が行われているため、予測モデルは、人種差別的な規範を強化します。

EMBERS（Early Model Based Event Recognition UsingSurrogates）は、進行中の組織活動を検出し、それに応じて**警告**を生成する。「世界の複数の地域」の「抗議行動、ストライキ、"オキュパイ" などの「社会不安事象」を予測するために使用。

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

標的を狙ったデータ収集

盗聴
CSS（Cell Site Simulator）：移動可能な小型の基地局で、周辺の携帯電話を CSS に接続して盗聴。

監視用のドローン
CSS　や高解像度ビデオカメラなどの監視機器を搭載して広域を監視。
令状による民間プロバイダーからの通信情報の取得

個人のスマホやパソコンへの攻撃
警察：勾留や捜索に際してデバイスを**押収・解析**
Cellebrite 社：イスラエルの企業。携帯電話その他のデバイスから**データを抽出するためのツール**を販売
NSO グループ：（これもイスラエルの企業）一部の iPhone やアンドロイドに　Pegasus　という**スパイウェアを遠隔操作でインストール**し、テキストメッセージや通話のメタデータ、パスワードなどのデータを抽出
NSA：データを収集したり、データがターゲットデバイスに到達するのをブロックしたりすることができる QUANTUM　と呼ばれる**マルウェア**（悪意のあるソフトウェア）を一揃い保有

デジタルによる社会運動の弾圧（米国の場合）

社会運動抑圧のメカニズム
社会運動に対するデジタルの脅威

個人的な嫌がらせ

Doxxing とは、標的となる人物の**個人情報**をディスカッションサイトなどで公開し、標的となる人物に危害を加えたり、困惑させたりすること

フィッシングとは、**偽装**された電子メールや Web サイトを通じて、パスワードなどの個人情報を入手する方法のこと

パスワード・スニッフィングは、あなたがパスワードを入力するのを肩越しに見るようなローテクなものから、キー・ストローク・ロガーをインストールしてあなたがパスワードを入力するキーボード操作を記録するようなものまであります。

社会運動を守るために

01 監視と抑圧から身を守る

監視相手があなたのデータを取得するための労力を増やすこと

02 セキュリティ文化

抑圧的な脅威による悪影響を最小限に抑える慣習をつくる

03 自分のデバイスを守る

携帯電話やノートパソコンに保存されているデータの防御

04 通信を守る

データ転送中の暗号化

05 リモートデータを守る

クラウド上のデータに誰がアクセスできるか

06 自分のアイデンティティを守るために

匿名と仮名、 Tor の使用方法

反対運動を防衛する　社会運動を守るために

監視と抑圧から身を守る / セキュリティ文化

監視と抑圧から身を守る

脅威　監視能力　抑圧リスク

$$\text{threat} \propto \frac{(\text{surveillance capabilities}) \times (\text{suppression risk})}{\text{effort required to obtain data}}$$

データ取得に必要な労力

監視能力(surveillance capabilities)とは、「社会運動に対するデジタルの脅威」の章で説明したように、相手のリソースのレベルを指します。抑圧リスクとは、相手がどのようにしてあなたを弱体化させようとするかということです。
留意すべきは、**監視が間接的にも直接的にも抑圧を支える**ということです。

すべきことは、
・脅威を軽減すること
・監視能力を低下させる
・弾圧のリスクを減らす
・データ取得にかかる労力を増やす

あなたのデータはどこに？
データの脆弱性がどこにあるかによって、あなたのデータ保護戦略が変わります。つまり、データが自分の**手元にあるスマホやパソコンの中にあるのか、リモートのクラウドにあるのか**、といったことを確認することが必要。

反対運動を防衛する　社会運動を守るために

監視と抑圧から身を守る / セキュリティ文化

セキュリティ文化

国家や民間の敵による密告者を使った弾圧の歴史を知っている社会運動では “セキュリティ文化” と呼ばれるものが発展しています。この言葉は、**グループとその活動、グループのメンバーや幅広い社会運動に対する侵入や監視などの抑圧的な脅威による悪影響を最小限に抑えることを目的とする情報共有の方法や行動上の注意事項**を意味します。

重要な原則

1.　情報は知る必要があるものだけを共有する。
情報の共有とデジタル化を最小限に抑える

2.　一緒に組織を作る場合、できるだけグループのメンバーをよく知ること。
データが暗号化されていないときは、そこへアクセスできるのが人間であろうと、インターネット・サービス・プロバイダーであろうと、クラウド・ストレージ・プロバイダーであろうと、メールプロバイダーであろうと、すべての対象についての**信頼性を確認しておく必要**があります。

3.　ゴシップやうわさ話を避ける。
ゴシップや噂に惹かれてしまう人間の弱点を国家は有利に利用してきました。**濡れ衣・挑発者・虚偽プロパガンダといった騙し戦術**が使われ、その情報を信じた社会運動のメンバーが情報拡散する、といったことが起きました。

反対運動を防衛する　社会運動を守るために

監視と抑圧から身を守る / セキュリティ文化 / 自分のデバイスを守る

自分のデバイスを守る

携帯電話やノートパソコンに保存されているデータは膨大です。連絡先、電子メール、写真、文書、カレンダー、確定申告書、銀行口座情報、そしてスマホの場合は、携帯電話を持っている間の位置情報の詳細な履歴も含まれています。これらのデータの多くは、クラウドストレージプロバイダー（ Apple 、 Google 、 Dropbox　など）とも共有されます。ここでは、ラップトップや携帯電話に保存されているデータを、遠隔地からの攻撃や実体的な攻撃から守ることに焦点を当てます。

実体的攻撃

紛失、盗難、没収などにより、敵対者がデバイスに直接にアクセスすること

リモート攻撃

インターネットやデータ接続を介して携帯電話やノートパソコンのデータに敵対者がアクセスすることを意味します。デバイス（スマホを対象とすることが多い）にマルウェアを感染させる機能を設計・販売している企業があり、その顧客（つまりあなたの敵対者、それが企業や国家のエージェントであっても）があなたの情報の一部または全部にリモートアクセスできるようにします。

対策

セキュリティの更新をかならずやること

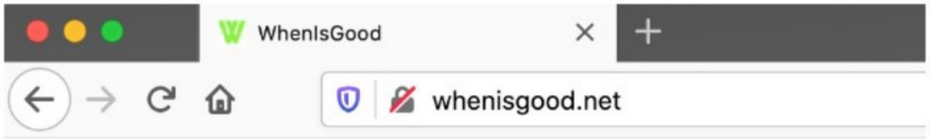
メールのリンクをクリックするときは十分に注意すること

反対運動を防衛する　社会運動を守るために

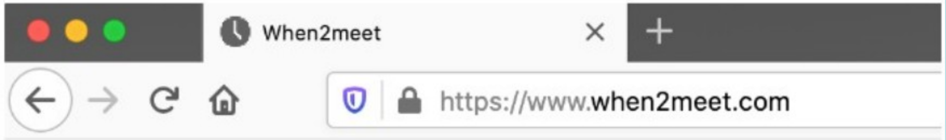
監視と抑圧から身を守る / セキュリティ文化 / 自分のデバイスを守る / 通信を守る

通信を守る

オンライン・コミュニケーションを保護する最善の方法は、暗号化です。
暗号化されているかどうか



HTTP, not encrypted



HTTPS, encrypted

（上図）HTTP、暗号化されていない　（下図）HTTPS、暗号化されている

データ転送中の暗号化

Assata　と通信プロバイダーのサーバー（センター）の間や、通信プロバイダーのサーバーと　Bobby　の間の経路にある盗聴者や通信機器を運用する業者は、あなたの通信内容にはアクセスできませんが（ただし、メタデータは取得できます）、**通信プロバイダーはあなたの通信内容にアクセスできる。**



In-transit encryption

データ転送中の暗号化

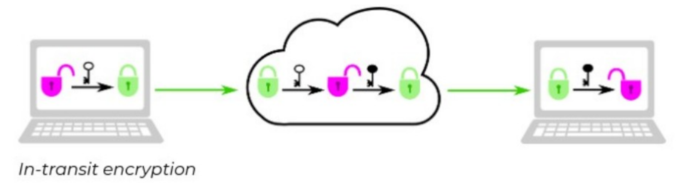
通信を守る（続）

エンド・ツー・エンドの暗号化

エンド・ツー・エンドの暗号化（ E2EE ）は、通信事業者からも通信を保護します。最下部の図は前ページの図。両方を比べてください。



ンド・ツー・エンドの暗号化



データ転送中の暗号化

認証

エンド・ツー・エンドの暗号化は、通信事業者（または通信経路上の第三者）が、**鍵交換の時点から中間者攻撃を受けていない場合にのみ成立**します。

アサタとボビーが独立したルートで鍵を確認すれば、中間者攻撃を受けていたかどうか、つまり通信が本当にエンド・ツー・エンドで暗号化されているのかを判断することができます。

反対運動を防衛する 社会運動を守るために

監視と抑圧から身を守る / セキュリティ文化 / 自分のデバイスを守る / 通信を守る / リモートデータを守る

リモートデータを守る

リモートに保存されている（そして暗号化されていない）データは、政府など敵対者が召喚状や令状によってアクセスできるほか、単なる第三者とも共有される可能性さえあります。残念なことに、最も明らかな形のリモートデータ保存（Dropbox や Google Drive など）を避けたとしても、私たちのデバイスの多くは、**内部データ全体のリモートバックアップ**を推奨しており（Apple デバイスの iCloud など）、場合によってはそれを避けることが非常に困難です（Android デバイスの Google アカウントなど）。これらのデータには、**アドレス、カレンダー、位置情報の履歴、閲覧情報など、あなたがコンピュータを使って行うあらゆる情報**が含まれています。

● Google は、あなたのすべての情報（メール、ファイル、連絡先、デバイスのバックアップ）を喜んで無料で保存します。もちろん、彼らはあなたのデータを利用することでそこから価値を引き出します。しかし、もしそのデータがあなただけが管理する鍵で暗号化されていれば、Google はあなたのデータを利用できません。

● CryptPad は、エンド・ツー・エンドで暗号化された Google Docs の代替となる共同編集プラットフォームです。

反対運動を防衛する　社会運動を守るために

監視と抑圧から身を守る / セキュリティ文化 / 自分のデバイスを守る / 通信を守る / リモートデータを守る / 自分のアイデンティティを守るために

自分のアイデンティティを守るために

Tor について
Tor　はあなたの身元に関する情報 (実際の場所など) を隠し、**匿名性や仮名性を得るために使用**することができます。初心者の場合、 Tor Browser　など　Tor　方式に対応したアプリを使って　Tor　システムを利用します。上級者では、 Tails　や　Whonix　などの　OS　を使うとあらゆる通信が　Tor　経由となり、もちろんウェブアクセスもすべて　Tor　経由になります。

Tor　ブラウザでは他のブラウザと同様に使用するだけで、あなたのユーザー名を使ったメールやソーシャルメディアへのアクセスを含め、あなたの物理的な位置をそれらのアカウントから隠すことができます。

Tor でも匿名性の確保ができない場合
・アカウントへのログイン (例 : ソーシャルメディア、電子メール、銀行など)
・自分のウェブサイトを繰り返し表示する

Tor　は匿名性を提供するだけであり、プライバシーを守るためには、 https　によるエンド・ツー・エンドの暗号化を使用したウェブページにアクセスする必要があることを覚えておいてください

暗号化とは何か？

暗号化とは、メッセージにスクランブルをかけて、意図した相手だけが解読（読み取り）できるようにするプロセスです。元のメッセージ（平文［ひらぶん］）をスクランブルする方法は、暗号または暗号化プロトコルと呼ばれます。

暗号文そのものは秘密にする必要はない。冷蔵庫のドアに貼り付けておいてもよい。

例：シーザー暗号

平文（ひらぶん）

IF VOTING CHANGED ANYTHING IT WOULD BE ILLEGAL(※)

暗号文

li yrwlqj fkdqjhg dqbwklqj lw zrxog eh loohjdo

メッセージの各文字を、申し合わせておいた数だけアルファベットをシフトさせます。上の例では、3文字後ろにずらします。

I ⇒ l に、F ⇒ i ...となります。

※ この言葉は、20世紀初頭の米国のアナキスト、エマ・ゴルドマンの言葉とされている。「投票で何かが変えられたとき、変えられた何かが違法なことになってしまうだろう」今まで合法だった事柄が議会の投票で違法とされてしまうことへの批判

現代の暗号技術

鍵が長いということは、正しい鍵を推測するために、より多くの可能性のある鍵を探さなければならないということです。時代が進み、コンピュータの処理が高速化・高性能化すると、ブルートフォース（総当たり）攻撃が不可能であることを保証するために、より長い鍵が必要になることがあります。

暗号方式は、**暗号の方法が公開されていても安全でなければならない**。⇒暗号の方法の公開とは、暗号方法の妥当性を誰もが検証できることを意味します。この「方法」を知っていることと、実際の暗号文を解読できることとは別のことです。

たとえば、下記の暗号文がシーザー暗号であることを知っていても直ちには解読できません。

li yrwlqj fkdqjhg dqbwklqj lw zrxog eh loohjdo

しかし、ちょっと努力すれば解読が可能です。AI に問い合わせれば一瞬で回答を寄せるでしょう。

なので、シーザー暗号のような仕組みは、遊びで使う以外に実用的な暗号としては使えません。

例　ヴィジュネル暗号

複数のシーザー暗号を組み合わせたもので、それぞれに鍵があります。

RESPECT EXISTENCE OR EXPECT RESISTANCE
(存在を尊重せよ、さもなくば抵抗に遭う)

ACT という単語で暗号化する。
RESPECT EXISTENCE OR EXPECT RESISTANCE

A を鍵にするので、移動は 0⇒ それぞれ、R、P、T となる

C を鍵にするので、移動は 3⇒ それぞれ、G、G、G となる

3 番目は T を鍵にするので、移動は 19⇒ それぞれ、L、V、Q となる (煩雑になるので→は省略)

ACT という鍵の意味は、

最初の平文の文字を A だけずらす。⇒アルファベット順で A から 0 番目なので、 0 だけずらす。⇒ A のまま
二番目の文字を C だけずらず。⇒アルファベット順で A から数えて 3 番目なので、 3 だけずらず。⇒ A ならに、 B なら D にずらす。
三番目の文字を T だけずらす。⇒同じく、アルファベット順で 19 番目なので、 19 だけずらす。

左の例のばあいは下記の暗号文になる。
rglpgvt gqiumepve qk ezieem rgliumapve

※鍵の単語は何でもよい。アルファベットである必要もない。

物理的な例。安全でないチャンネルでの秘密の合意

暗号化されたメッセージを解読するには「鍵」の共有が不可欠になる。

右図の紫色が秘密の色 (秘密の鍵に該当)。この秘密の色を教えあったりせず、第三者にも知られずに、二人が共有できる方法がある。

仮定 1． 2 色の絵の具を混合し、混合された絵の具からもとの二つの色に戻すことはできないと仮定。

仮定 2． 二つの色のうちのひとつの色だけを知っているとして、それに何の色を混ぜて、結果的に混ざった色になったのかを知ることはできないと仮定。

アサタとボビーは、絵の具の色 (黄色) と量 (10mL) に安全ではない通信経路で合意 (1)。**盗聴者もこの情報を知る**。

ササタは秘密の赤茶色 (2) を加え、オレンジ色を作る (3)。

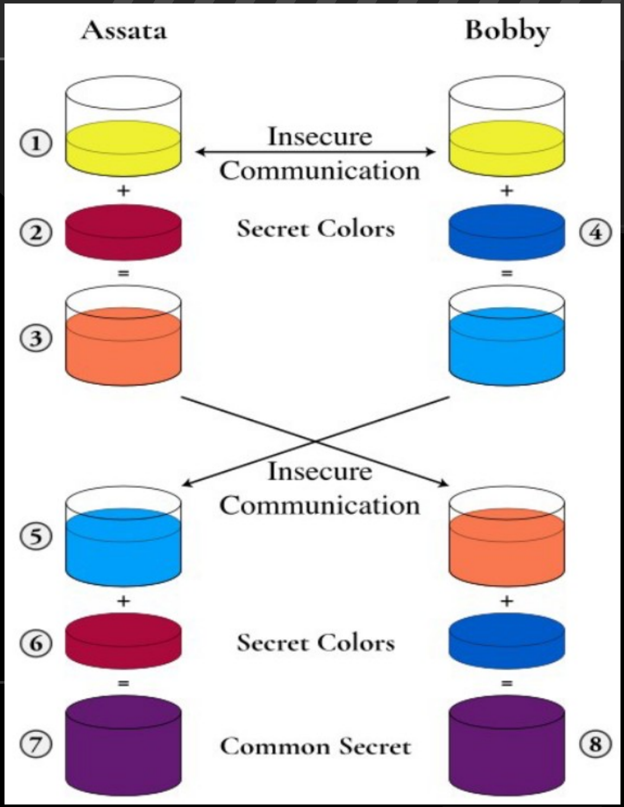
ボビーは黄色 (1) に秘密の青色 (4) を加えて空色を作る。

お互いに作成した色の絵の具を、**盗聴者に知られるなかで交換**。

アサタはボビーから送られた絵の具に秘密の赤茶色を加えて紫色を作る (7)

ボビーも送られてきた色に秘密の青色を加え紫色を作成 (8)

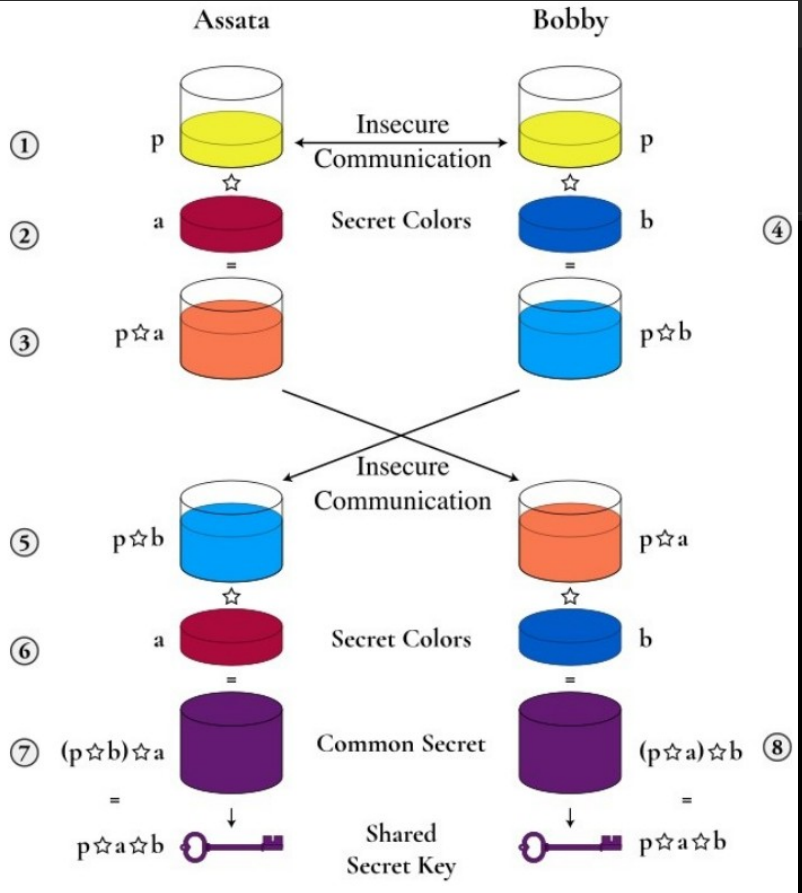
盗聴者は、アサタとボビーの秘密の色がわからなければ、紫色を作ることはできない。⇒ ディフィー・ヘルマン鍵交換



ディフィー・ヘルマン鍵交換（Diffie-Hellman Key Exchange）

このプロセスを数学的に再検討してみましょう。ここでは、元に戻すことは不可能か困難で、しかも可換式の数学的操作を用います。逆転が困難な数学的演算や関数は一方向性関数と呼ばれます。この数学的操作を記号☆で表す。

アサタとボビーがある数字　p　に合意し、それを公開（1）します。アサタは秘密の数 a を選び（2）、 p☆a を計算し（3）、その結果をボビーに送ります。ボビーは秘密の数字 b を選び（4）、 p☆b を計算して、その結果をアサタに送ります（5）。アサタはボビーからのメッセージ（5）と自分の秘密番号（6）を使って、（p☆b）☆a(7）を計算します。ボビーは、アサタからのメッセージ（3）と自分の秘密の番号（4）を使って、（p☆a）☆b(8）を計算します。☆は可換なので、（p☆b）☆a=(p☆a）☆b となり、アサタとボビーがそれぞれ計算しても、同じ結果になる。盗聴者は p☆a 、 p☆b 、それに p しか知らず、☆は一方通行なので、盗聴者はアサタとボビーの共有共通番号を計算する効率的な手段を持っていません。それはアサタとボビーの秘密です。アサタとボビーは、この共有する数を暗号鍵として使用することができます。

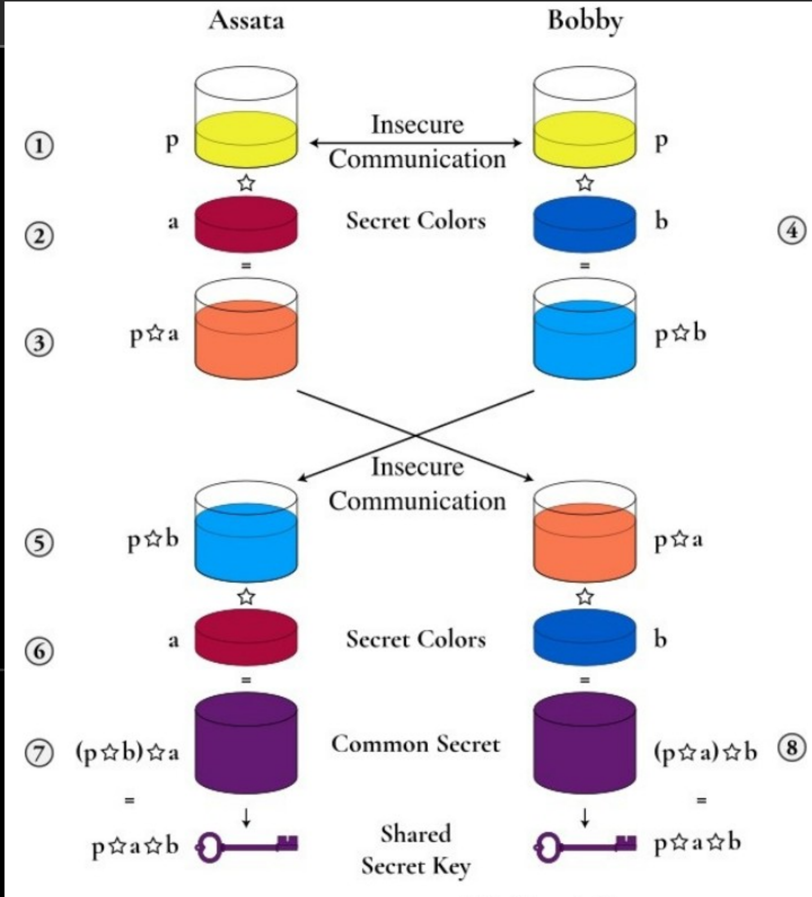


秘密鍵の合意

ディフィー・ヘルマン鍵交換の利用

ディフィー・ヘルマン鍵交換は、暗号鍵を合意するための手段としてあちこちで使用されています。この鍵交換は、皆さんが遭遇するほとんどの暗号化通信の基礎として使用されています。特に、**https でWeb サイトに接続する際の鍵交換の基本となっています。**あなたがウェブサイトにアクセスするとき、URL は http:// または https:// で始まります。前者の場合、ウェブサイトのサーバーとの通信は一切暗号化されません。後者の場合、通信は暗号化され、その通信を暗号化するための鍵はディフィー・ヘルマン鍵交換で生成されます。

https では、自分のデバイスとウエッブサイトとの間で、データを暗号化して通信を行なうことで、通信回路での盗聴を阻止する。このときに、盗聴者に知られることなく暗号化の秘密鍵を両者で共有する必要がある。この鍵を生成する方法としてデフィー・ヘルマン鍵交換が用いられる。



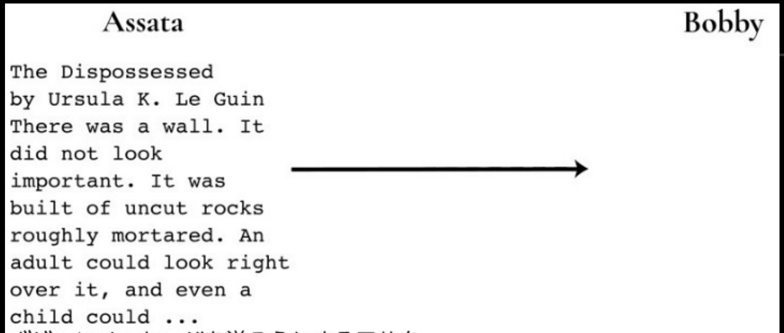
秘密鍵の合意

暗号化キーの保護によるセキュリティの確保

最近の暗号プロトコルでは、暗号化方式が一般的に公開されているため、セキュリティを確保するには、暗号化キーを保護する必要があります。実際にどのように保護するかは、暗号鍵がどこにあるかによって異なります。安全なインスタントメッセージングアプリである Signal の場合、暗号化キーは携帯電話内のファイルで、これが携帯電話の通信を保護しています。あなたのパスワードをクラウドと同期できるようなパスワード・マネージャーの場合、あなたのパスワードを全部保存しているファイルを暗号化する鍵は、パスワード・マネージャーにログインするときのパスワードから導出され保護されていています。

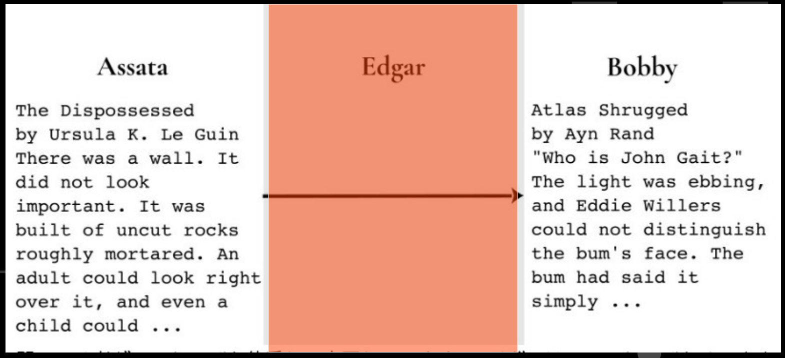
インフラへの不信感がセキュリティにつながる

エンド・ツー・エンドの暗号化とは、メッセージは通信回路の中間では読めず、エンドポイント（終点）でしか読めないようにすること。エンド・ツー・暗号化されていないと ...



ボビーにメッセージを送ろうとするアサタ

エドガーがアサタからの通信を盗聴し、さらにメッセージ内容を改竄する

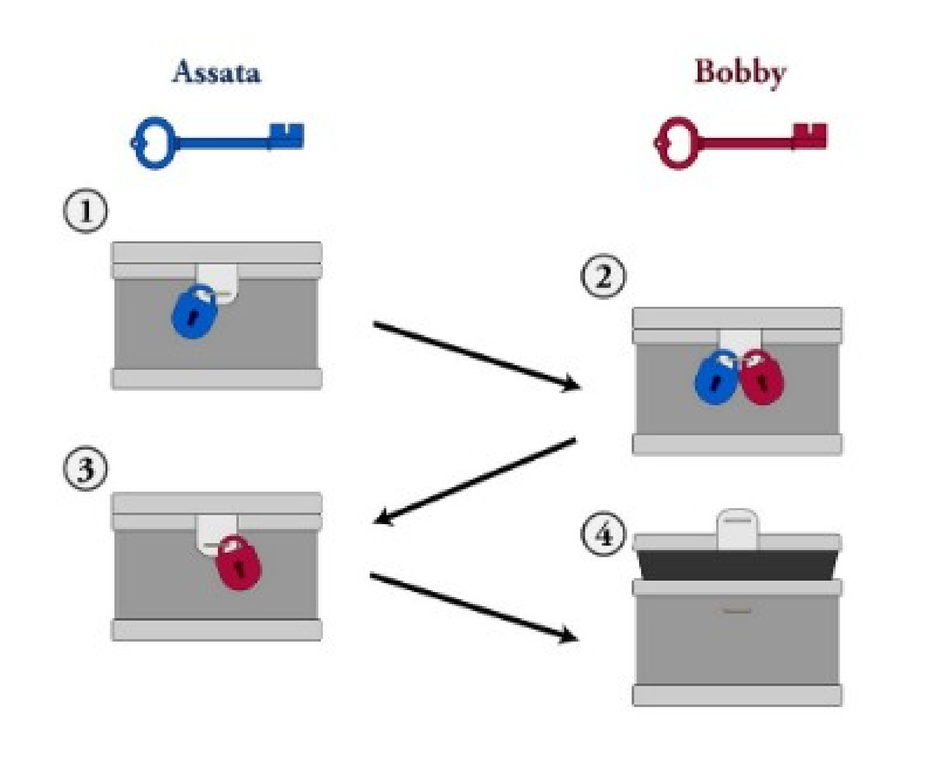


※アサタのテキストはアーシュラ・K・ルグィンのアーシュラ・K・ル・グィンの『所有せざる人々』（早川書房）、エドガーはかわりに、右翼好みのアイン・ランドの『肩をすくめるアトラス』（日本語版、アトランティス）を送っている。

鍵を交換なしで秘密のメッセージを送る方法 (実世界のばあい)

1. アサタは自分の荷物に自分の鍵でロックする。
2. ボビーは、届いた荷物に追加で自分の鍵で更にロックして、アサタに荷物を返送する。
3. アサタは自分のロックを自分の鍵で外し、再度ボビーに荷物を送る。 (しかしボビーの鍵でロックされているので荷物は開けられない)
4. ボビーは届いた荷物のロックを自分の鍵で開錠する。

第三者に読まれないように通信するには、同じことを通信環境で実現することになる。



暗号化ハッシュ

ハッシュ関数とは、任意の大きさのデータ（名前、文書、コンピュータプログラムなど）を、固定の大きさのデータに変換する（コンピュータの）関数のこと

1． 同じメッセージは常に同じ出力ハッシュになる。

2． 入力メッセージから出力ハッシュ値を生成することは、ブルート・フォース（可能な入力メッセージをすべて試す）以外では不可能である。

3． 同じ出力ハッシュ値になる2つの異なる入力メッセージを見つけることは不可能である。

4． 入力メッセージへの小さな変更は、新しいハッシュ値が元のハッシュ値と無相関に見えるほど、出力ハッシュ値が大きく変化する。

暗号化は、復号鍵を使って、暗号文から平文へと遡ることができますが、ハッシュ関数は本質的に一方通行であり、逆のことができるための鍵はありません。暗号ハッシュ関数の出力は、（暗号文のように）入力メッセージのすべての情報を暗号化しているわけではありませんが、入力を識別するのに十分な情報を暗号化しており（性質 1 と 3 に依存）、これを偽造することは極めて困難です（性質 2）。

暗号化ハッシュの例え話

アサタとボビーの二人が難しい数学の問題を解こうとしています。アサタは問題を解いたことを、解答を示さずにボビーに伝えるときに暗号化ハッシュを使う。

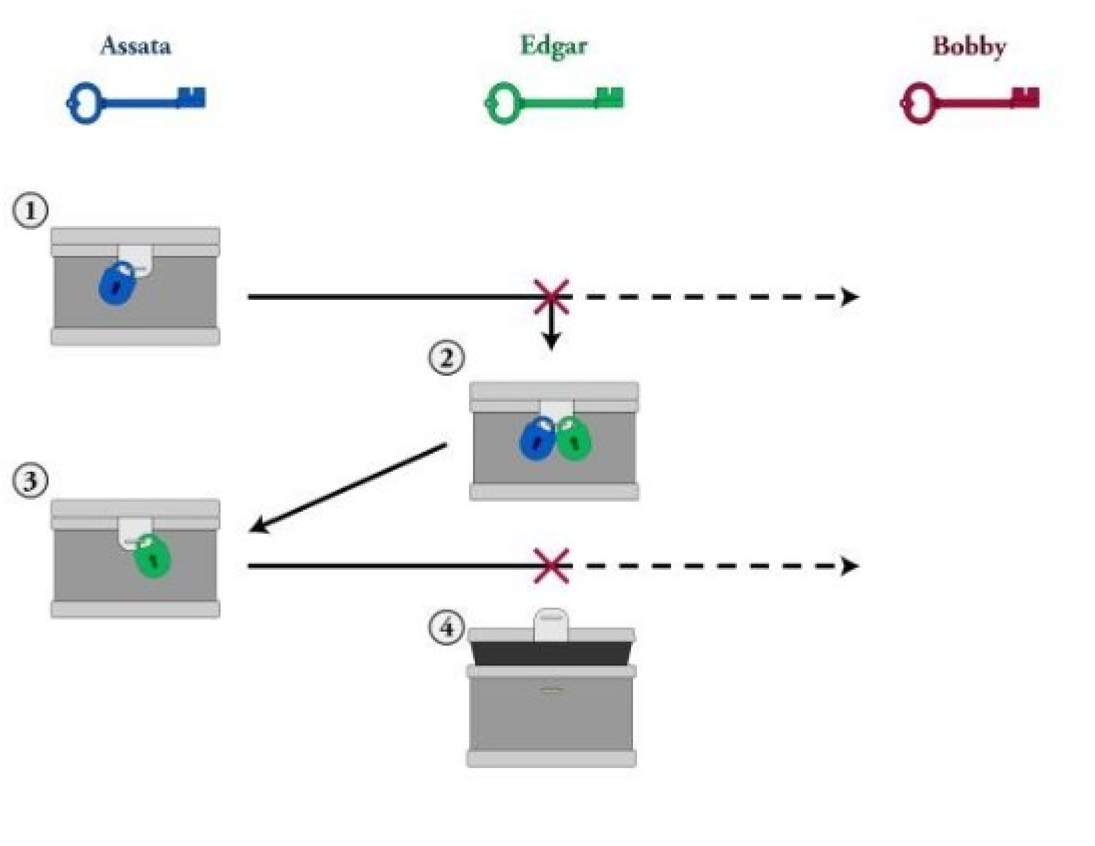
(1) アサタは自分の解答を暗号化ハッシュ hash(S) をボビーに伝える。

(2) ボビーは遅れて問題の解答を得る。

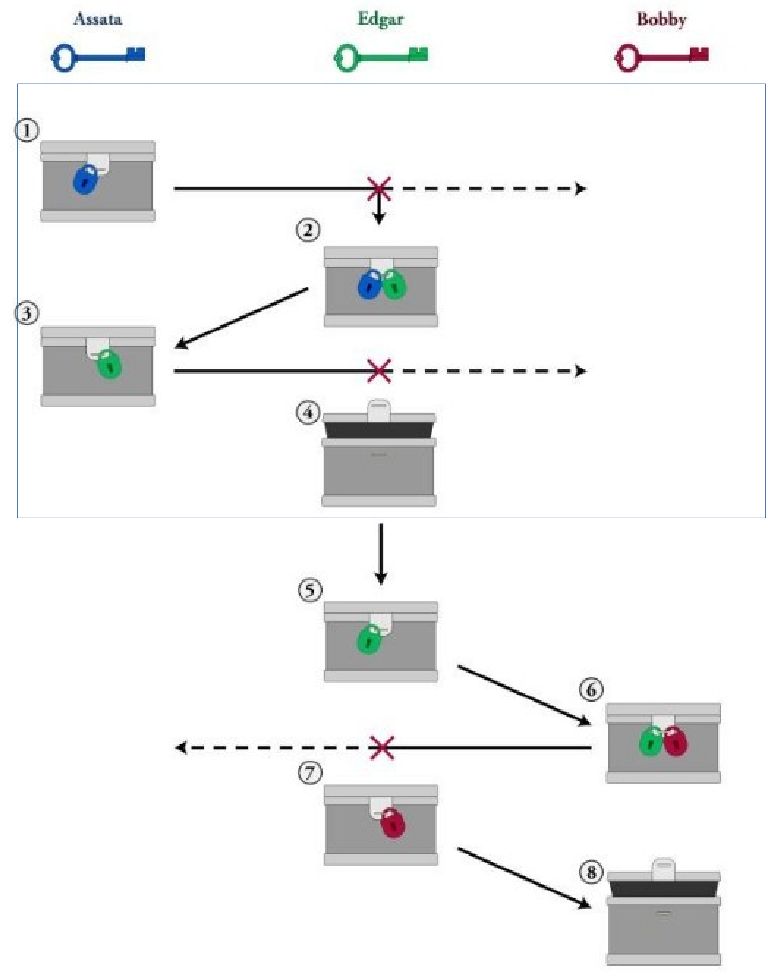
(3) ボビーは自分の解答を暗号化ハッシュにする。

(4) ボビーの暗号化ハッシュとアサタから送られてきた暗号化ハッシュが一致すれば、アサタの方が早く解答したことが証明されることになる。

なりすまし攻撃と中間者攻撃

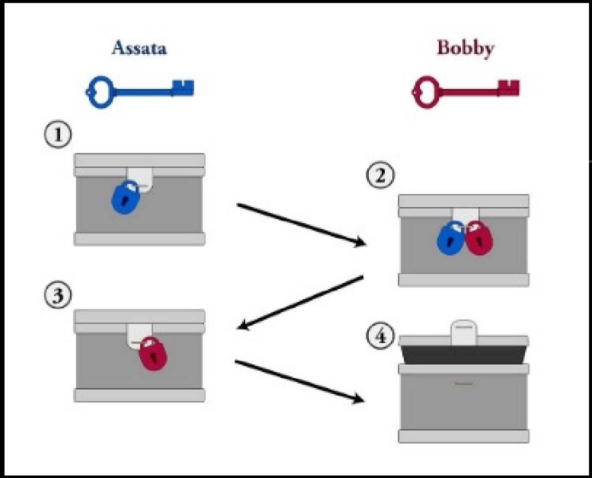


なりすまし攻撃

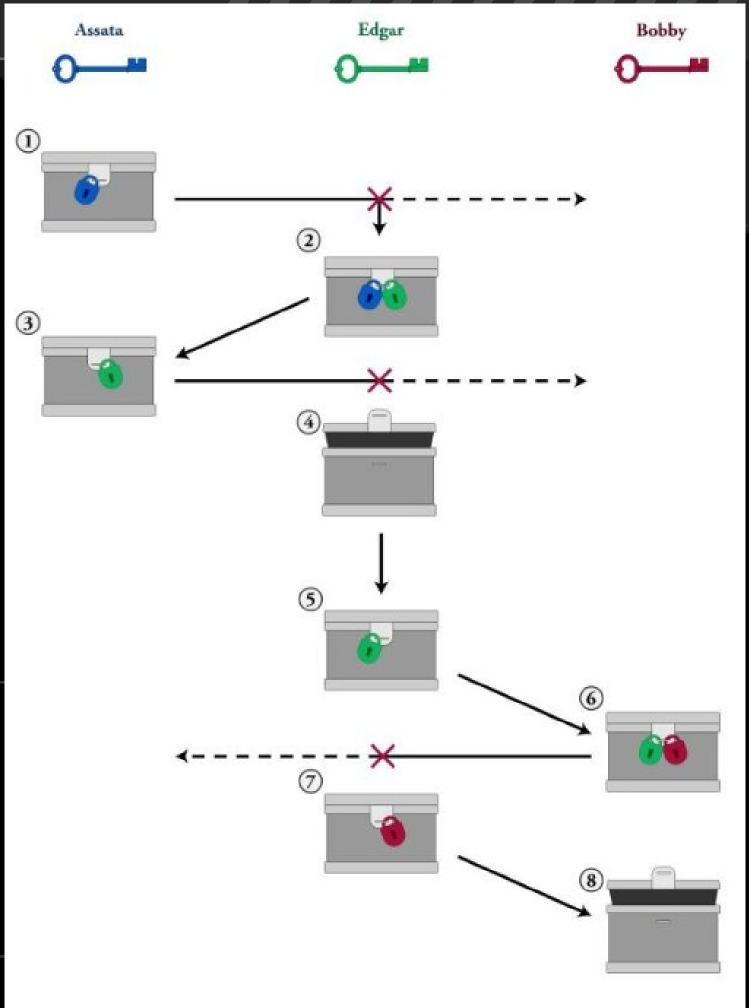


中間者攻撃

なりすまし攻撃と中間者攻撃

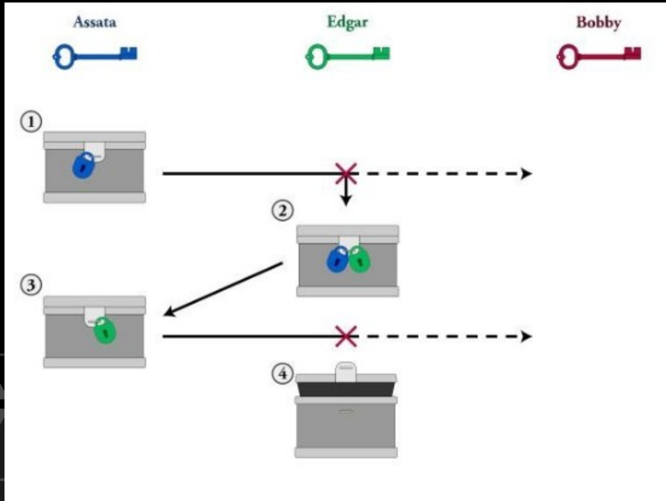


エドガーがアサタにもなりすましてボビーと通信。

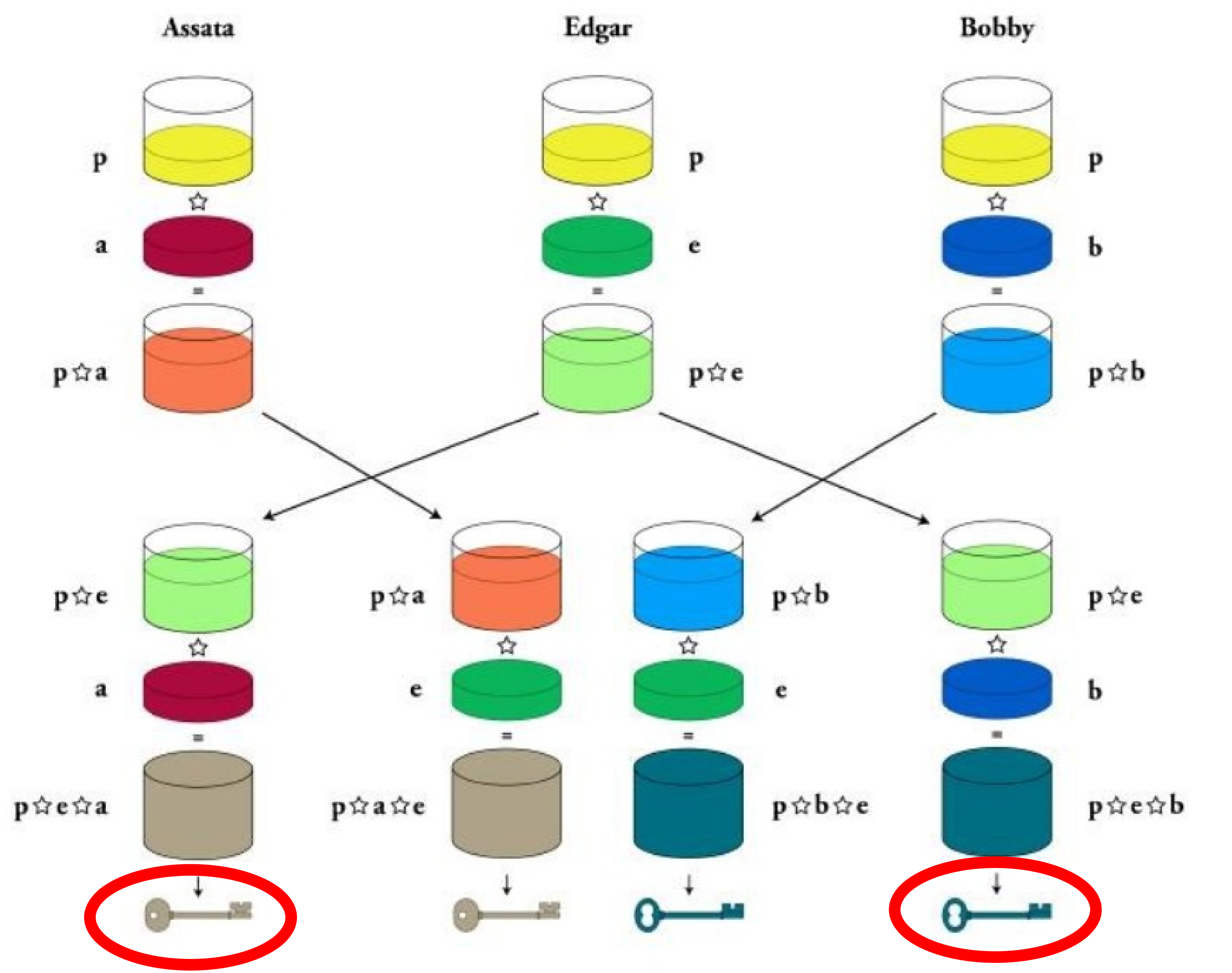


中間者攻撃

エドガーがボビーになりすまして通信。



なりすまし攻撃



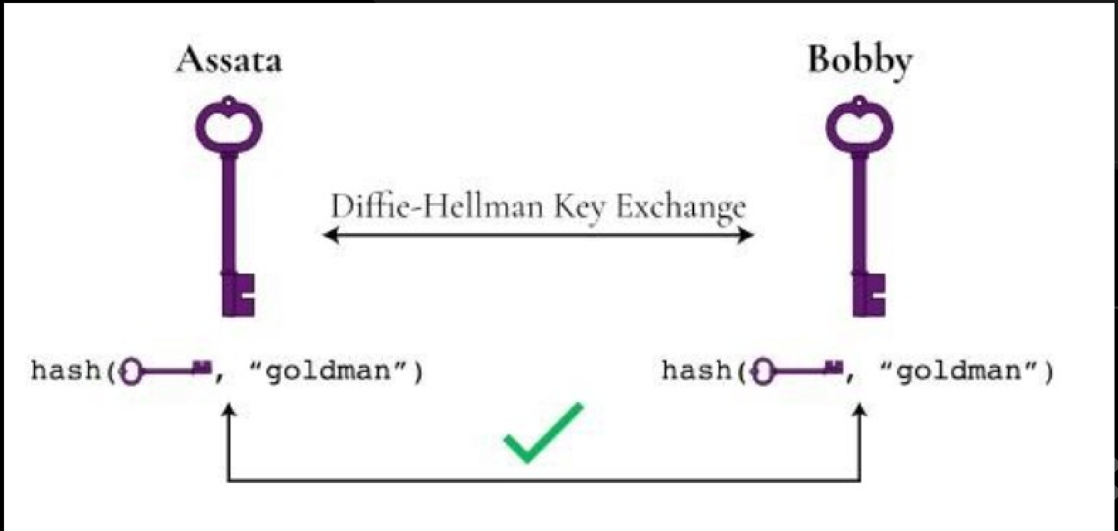
ディフィー・ヘルマン鍵交換に対する中間者攻撃

ディフィー・ヘルマン鍵交換に対する中間者攻撃

左図のようにすれば、エドガーはアサタとボビーの間で通信を傍受したり改竄できるが、両者の通信を継続的に傍受しなければ、「鍵」が違うことがバレてしまい、中間者の存在が知られてしまう。

暗号ハッシュによる中間者攻撃の発見：フィンガープリンティング

アサタとボビーがディフィー・ヘルマン鍵交換を行った後、２人の鍵を比較して同じ鍵であることが確認できれば、盗聴者が中間者攻撃を行っておらず、２人だけが暗号化された通信を見ていることが確認できます。



フィンガープリンティング

結論
デジタルセキュリティツールの選択

01 必須の基準

1. エンド・ツー・エンドの暗号化
2. 中間者攻撃を防ぐ機能
3. オープンソースを選択
4. アプリの真正性を暗号署名で検証できる

02 追加の望ましい技術的基準

1. デジタル・セキュリティ・ツールは、クロスプラットフォームが望ましい
2. セキュリティ監査を受けている
3. 匿名性や仮名性を提供している
4. ツールの設定確認（暗号化が選択できれば、選択する）
5. ピア・ツー・ピア通信やフェデレーション機能の利用（中央集権的に特定の企業がサーバーを管理しない仕組、あるいはサーバーを介さない仕組み）

03 技術以外の基準

1. プロバイダが採用した財務モデル。あるツールが無料で使えるとしたら、その理由を知るべき
2. ツールが運動志向の場合、それはプラスにもマイナスにもなり得ます。サーバーの運営主体が社会運動団体の場合は、サーバー内での暗号化ができていなくても信頼性が高い。（riseup の jitsi-meet）
3. 事業者の透明性

Thank You!

:)